IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN
GREEN BAY DIVISION

IN RE FOREFRONT DATA BREACH LITIGATION This Document Relates to: ALL ACTIONS	Master File No. 1:21-cv-00887-LA

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs JUDITH LEITERMANN, LYNN ANDERSON, and MILAN E. KUNZELMANN, ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action lawsuit against FOREFRONT DERMATOLOGY, S.C., a Wisconsin service corporation, and FOREFRONT MANAGEMENT, LLC, a Delaware Limited Liability Company (collectively, "Forefront" or "Defendants") to obtain damages, restitution, and injunctive relief for the Class, as defined below. Plaintiffs allege the following upon information and belief, except as to their own actions, the investigation of their counsel, and certain facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action lawsuit arises out of a targeted ransomware cyberattack and data breach (the "Data Breach") that occurred at Forefront, a dermatology group practice comprised of more than 210 board-certified dermatologists practicing in over 195 locations in 22 states.

2. As a result of the Data Breach, Plaintiffs and approximately 2,413,552 current and former patients and employees of Forefront ("Class Members") were harmed in the form of the loss of the benefit of their bargain, out-of-pocket expenses, loss of privacy, and loss of the value of their time reasonably incurred to remedy or to mitigate the effects of the attack.

3. Through its public statements, Forefront attempted to minimize the breadth and

severity of the Data Breach, not to mention its own negligence in allowing the breach to happen in the first place.

4. For instance, although Forefront reported the Data Breach to the Maine Attorney General's Office as affecting "only" 4,431 persons,[1] Defendants reported the Data Breach to the United States' Department of Health and Human Service's Office for Civil Rights as affecting 2,413,553 persons.[2]

5. Moreover, in a "Notice of Data Security Incident" (the "Notice") posted on its website, Forefront described the incident as an "intrusion into its IT network by unauthorized parties and determined that the incident resulted in unauthorized access to certain files on its IT systems that contain Forefront patient information."[3]

6. Forefront neglects to mention that the intrusion was possible (and certainly foreseeable) because of its inadequate data security protocols, including incredibly simplistic passwords.

7. As a result of Defendants' failure to employ adequate data privacy and security measures, Plaintiffs' and Class Members' sensitive personal information—which was entrusted to Defendants—was exposed, compromised, and unlawfully accessed.

8. Although the list is likely non-exhaustive, Forefront has acknowledged that the information compromised in the Data Breach includes patient names, addresses, dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers,

---

1 *See* https://apps.web.maine.gov/online/aeviewer/ME/40/f3f9c506-728b-4271-9497-95ce115e2fd0.shtml (last visited February 14, 2022).

2 *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited February 17, 2022); *but see also* https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/ (last visited February 15, 2022).

3 https://forefrontdermatology.com/incidentnotice/ (last visited February 15, 2022).

dates of service, accession numbers, provider names, and/or medical and clinical treatment information, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Forefront collected and maintained (collectively, the "Private Information").

9. While Forefront proclaims in the Notice it posted on its website that "there is no evidence that patient Social Security numbers, driver's license numbers, or financial account/payment card information were involved in this incident," that representation is contradicted by its own statements to the Maine Attorney General:

> Information Acquired - Name or other personal identifier in combination with: Social Security Number[4]

10. Moreover, the Notice of Data Breach that Forefront submitted to the California Attorney General's Office states that it "could not rule out the possibility that files containing some of your information, including your name and Social Security number, may have been subject to unauthorized access as a result of this incident."[5]

11. Accordingly, Plaintiffs brings this class action lawsuit to address Forefront's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiffs and Class Members that their information had been subject to unauthorized access by a third party (threat actors calling themselves Cuba Ransomware) and precisely what specific type of information was accessed.

12. Forefront maintained the Private Information in a reckless manner. In particular,

---

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/f3f9c506-728b-4271-9497-95ce115e2fd0.shtml (last visited February 15, 2022).

[5] https://oag.ca.gov/system/files/FFM FFD - California Notification.pdf (last visited February 15, 2022).

the Private Information was maintained on Forefront's computer network in a condition vulnerable to cyberattacks, such as the one that occurred in late May to early June of 2021 thereby enabling access to Defendants' network and, ultimately, to the Private Information.

13. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Forefront, and thus it was on notice that failing to take appropriate steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

14. In addition, Forefront failed to properly monitor the computer network and systems that housed the Private Information; had Forefront properly monitored its property, it would have been able to prevent or, at least, to discover the intrusion sooner.

15. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

16. According to a Databreaches.net article, "some of Forefront Dermatology's files remain freely available on the Cuba Ransomware leak site."[6]

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's

[6] https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/ (emphasis added).

licenses in Class Members' names but with another person's photograph and/or giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and to detect identity theft.

19. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs and injunctive relief including improvements to Forefront's data security systems, future annual audits and adequate credit monitoring services funded by Defendants.[7]

PARTIES

20. Plaintiff Judith Leitermann is, and at all times mentioned herein was, an individual citizen of the state of Wisconsin residing in the city of Neenah, Wisconsin. Plaintiff Leitermann was notified of Defendants' Data Breach and her Private Information being compromised upon receiving a letter titled "Notice of a Data Breach" dated as of July 8, 2021.

21. Plaintiff Lynn Anderson is, and at all times mentioned herein was, an individual

[7] While not mentioned on the Notice on its website, Forefront is evidently making a complimentary 12-month membership to TransUnion's *my*TrueIdentity Credit Monitoring Service available to affected individuals. *See* https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf. For the reasons set forth herein, such an offer is wholly inadequate under the circumstances and in no way obviates the need for this Court to fashion appropriate and meaningful injunctive relief on behalf of the millions of impacted individuals.

citizen of the commonwealth of Pennsylvania residing in the city of Pittsburgh. Plaintiff Anderson was notified of Defendants' Data Breach and her Private Information being compromised upon receiving a letter titled "Notice of a Data Breach" dated as of July 8, 2021.

22. Plaintiff Milan E. Kunzelmann is, and at all times mentioned herein was, an individual citizen of the state of Missouri residing in the city of Camdenton. Plaintiff Kunzelmann was notified of Defendants' Data Breach and his Private Information being compromised upon receiving a letter titled "Notice of a Data Breach" dated as of July 8, 2021.

23. Forefront Dermatology, S.C., a Wisconsin service corporation, is a dermatology group practice comprised of more than 210 affiliated board-certified dermatologists practicing in over 195 locations in 22 states.[8]

24. Forefront Management, LLC is a Delaware Limited Liability Company registered to do business in Wisconsin.

25. Defendants maintain their corporate offices at 801 York Street in Manitowoc, Wisconsin 54220.

26. Defendants can be served through their registered agent, CT Corporation System, 301 S. Bedford Street, Suite 1 in Madison, Wisconsin 53703.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, Pub. L. No. 109-2 Stat. 4 ("CAFA"), which, *inter alia*, amends 28 U.S.C. § 1332, at new subsection (d), conferring federal jurisdiction over class actions where, as here: (a) there are 100 or more members in the proposed class; (b) some members of the proposed Class have a different citizenship from Defendants and (c) the claims of the proposed class

[8] *See* https://forefrontdermatology.com/ (last visited February 15, 2022).

members exceed the sum or value of five million dollars ($5,000,000) in aggregate. *See* 28 U.S.C. § 1332(d)(2) & (6).

28. This Court has personal jurisdiction over Defendants because (i) Forefront Dermatology, S.C. is a Wisconsin service corporation with its principal place of business in Manitowoc, Wisconsin and Forefront Management, LLC is a Delaware Limited Liability Company registered to do business in Wisconsin with its principal place of business in Manitowoc, Wisconsin, (ii) they committed tortious acts in Wisconsin and (iii) they have sufficient minimum contacts and have engaged in significant business activity in the state of Wisconsin.

29. Venue is proper in this judicial district pursuant to 18 U.S.C. §§ 1965(a) and (b) because Defendants have their principal place of business in Manitowoc, Wisconsin, regularly transact business within the geographic boundaries of this District and because the facts and circumstances giving rise to the claims asserted herein occurred within this District.

COMMON FACTUAL ALLEGATIONS

A. Forefront's Representations Regarding the Privacy and Security of Its Patients' and Employees' Confidential and Protected Information

30. Forefront Dermatology, S.C., a Wisconsin service corporation, is a dermatology group practice comprised of more than 210 board-certified dermatologists practicing in over 195 locations in 22 states.[9]

31. In the ordinary course of receiving treatment and health care services from Forefront, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Financial account information;
- Payment card information;

[9] *See* https://forefrontdermatology.com/ (last visited February 15, 2022).

- Medical histories;
- Treatment information;
- Medication or prescription information;
- Provider information;
- Address, phone number and email address and
- Health insurance information.

32. Additionally, Forefront may obtain private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends and/or family members, not to mention the tremendous amount of (current and former) employee information that it possesses.

33. Due to the highly sensitive and personal nature of the information it acquires and stores with respect to its patients, Forefront makes a "Notice of Privacy Practices" available to all patients via its website.

34. By that notice, Forefront acknowledges that "[i]t is your right as a patient to be informed of Forefront Dermatology's legal duties with respect to protection of the privacy of your protected health information ('PHI')."[10]

35. Moreover, Forefront, in its privacy policy, states

> Forefront Dermatology and its affiliates [] respect your privacy and are committed to protecting it through our compliance with this policy.

36. Finally, in its Notice of Data Breach, Forefront states that it "is committed to protecting the confidentiality and security of our current and former employees' information."[11]

37. Thus, as stated in its Notice of Privacy Practices, in its Privacy Policy, and in its Notice of Data Breach, Forefront promises to maintain the confidentiality of patients' health,

---

[10] https://forefrontdermatology.com/wp-content/uploads/2021/05/Forefront-Dermatology-Affiliated-Practices-NOPP-1.pdf (effective as of April 23, 2021 & last visited February 15, 2022).

[11] https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf.

financial and non-public personal information, ensure compliance with federal and state laws and regulations and to notify patients of any breach that jeopardizes their private information.

38. Specifically, in a section titled "Data Security," Forefront states:

> We implement a variety of security measures for the Website to maintain the safety of your personal information from any loss, misuse or change of information that is under our control. *Such security measures include firewalls, access restrictions and password protection.*
>
> We offer the use of a secure server. All supplied sensitive/credit information is transmitted via Secure Sockets Layer (SSL) technology and then encrypted into our payment gateway provider's database only to be accessible by those authorized with special access rights to such systems, and are required to keep the information confidential. After a transaction, your credit card information will not be stored on our servers. All other information collected through the Website will be retained for the length of time permitted by law. Personal identifiable information can be removed from our database at your request however we will retain non-personal identifiable information indefinitely.[12]

39. As a condition of receiving medical care and treatment at its facilities, Forefront requires that its patients entrust it with highly sensitive personal information.

40. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Forefront assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized access and/or disclosure.

41. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

42. Plaintiffs and the Class Members relied on Forefront to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only and to make only authorized disclosures of this information.

---

[12] https://forefrontdermatology.com/privacy-policy/ (emphasis added) (last visited February 15, 2022).

B. Threat Actors Are Able to Access and to Make Confidential Health and Other Protected Information Publicly Available Due to Forefront's Lax Data Security Practices

43. According to its Notice of Data Security Incident, on June 24, 2021, Forefront Dermatology, S.C. and its affiliated practices concluded its investigation of an intrusion into its IT network by unauthorized parties and determined that the incident resulted in unauthorized access to certain files on its IT systems that contain patient information.

44. Subsequent investigation revealed that there had been unauthorized access to patient files and employee files between the dates of May 28, 2021 and June 4, 2021.

45. Forefront's Notice does not mention any specific ransom demand or whether they negotiated at all with the threat actors. Although not revealed in their disclosure, the attack was the work of threat actors calling themselves "Cuba Ransomware."

46. On information and belief, some of Forefront's files remain freely available on the Cuba Ransomware leak site.[13]

47. The threat actors dumped some of Forefront's data, including some patient information, at the end of the June 2021. Also included in that dump "was more than 130 files with information on [Forefront's] system and network, with security and backup details, and all their logins to health insurance portals, etc."[14]

48. A passwords file in the dump listed more than 100 sets of logins:

> Sadly, there was what appeared to be a lot of weak password and extensive password reuse. More than 40 passwords had "Forefront" in combination with some digit(s) and an exclamation point. Another 10 had some variant of DAWderm1![15]

---

13 https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/

14 *Id.*

15 *Id.*

49. Passwords and email addresses with security questions used for one insurer's portal revealed significant re-use:

User	User Name	Password	Security Questions	Email address
[redacted]	[redacted]	dawderm3	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	[redacted]
		dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		600York	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		Dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		forefront4!	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		dawderm1	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	
		Forefront1!	What is your mother's maiden name? **derm1** What is your father's middle name? **derm2**	

50. As acknowledged by Forefront, this information may have included patient names, addresses, dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, accession numbers, provider names, and/or medical and clinical treatment information.[16]

51. Not publicly acknowledged by Forefront is that the compromised information may have included Social Security numbers.[17]

52. While only some of the stolen information has been dumped on the internet to date, the threat actors appear to have exfiltrated a large amount of data, meaning additional dumps of Plaintiffs' and the Class Members' confidential and other private information are certainly possible and likely.

16 https://forefrontdermatology.com/incidentnotice/.

17 https://oag.ca.gov/system/files/FFM%20FFD%20-%20California%20Notification.pdf.

53. Upon information and belief, the cyberattack targeted Forefront due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI, and the targeted attack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients and employees like Plaintiffs and the Class Members.

54. Because of this cyberattack, data thieves were able to gain access to and exfiltrate the protected Private Information of millions of Forefront patients and (current and former) employees.

55. Though Forefront impliedly acknowledges that its system was inadequate to prevent such a cyberattack (and thereby protect the confidential Private Information it swore to protect), it is only offering a complimentary twelve-month membership of identity monitoring services for victims.

56. The offer of identity monitoring services is inadequate, but is an acknowledgment by Forefront that the impacted customers are subject to a substantial and present threat of fraud and identity theft.

C. Forefront Was Well Aware of the Risk of a Data Breach

57. Forefront had obligations created by HIPAA, contract, industry standards, common law as well as its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

58. Plaintiffs and Class Members provided their Private Information to Forefront with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

59. Forefront's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the

date of the breach.

60. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), among others, Forefront knew or should have known that its electronic records would be targeted by cybercriminals.

61. In fact, as of mid-2021 there were over 220 data breach incidents.[18] These approximately 220 data breach incidents impacted nearly 15 million individuals.[19]

62. Indeed, cyberattacks have become so prevalent that the Federal Bureau of Investigation and the United States Secret Service have issued a warning to potential targets such as healthcare providers like Forefront so they are prepared for a potential attack.

63. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[20]

64. According to the cybersecurity firm Mimecast, 90% of healthcare organizations

---

[18] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/ (last visited February 15, 2022).

[19] *Id*.

[20] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited February 15, 2022).

experienced cyberattacks in the past year.[21]

65. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the medical and healthcare industries, including Defendants.

66. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with data security standards.[22]

67. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Forefront failed to take reasonable steps to bolster its data security and adequately protect against the Data Breach and exposure of Plaintiffs' and Class Members' Private Information, leaving patients and employees exposed to an imminent risk of fraud and identity theft.

68. The risk of harm is indeed imminent under the circumstances presented by the Data Breach. As the Seventh Circuit has noted, the Data Breach presents circumstances such that there is "no need to speculate as to whether [class members'] information has been stolen and what information was taken." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (citation omitted). In *Remijas,* the Seventh Circuit explained how breach victims are harmed under the circumstances Forefront's patients and employees are facing:

[T]he [impacted] customers should not have to wait until hackers commit identity

---

[21] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited February 15, 2022).

[22] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited February 15, 2022).

> theft or credit-card fraud in order to give the class standing, because there is an "objectively reasonable likelihood" that such an injury will occur. Requiring the plaintiffs "to wait for the threatened harm to materialize in order to sue" would create a different problem: "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach." . . . At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the . . . data breach. *Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.*

794 F.3d at 693 (emphasis added).

69. Forefront is, and at all relevant times has been, aware that the Private Information it collects in connection with providing dermatology services is highly sensitive, and it was aware of the importance of safeguarding that information and protecting its IT systems from security vulnerabilities.

70. Forefront was aware, or should have been aware, of regulatory and industry guidance regarding data security, and it was alerted to the risk associated with failing to ensure that Private Information was adequately secured.

71. Despite the well-known risks of hackers and cybersecurity intrusions, Forefront failed to employ adequate data security measures in a meaningful way, or make changes to its practices and protocols, in order to prevent breaches, including the Data Breach, impacting and exposing sensitive Private Information.

72. Had Forefront adequately protected and secured its IT systems and Class Members' Private Information, it could have prevented the Data Breach.

73. Forefront permitted Plaintiffs' and Class Members' Private Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

D. Defendants Fail to Comply with FTC Guidelines

74. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

75. According to the FTC, the need for data security should be factored into all business decision-making.

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities and implement policies to correct any security problems.[23]

77. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.[24]

78. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.

---

[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited February 15, 2022).

[24] *Id*.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. These FTC enforcement actions include actions against healthcare providers like Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

81. Defendants failed to properly implement basic data security measures to protect against unauthorized access to patient PII and PHI, which constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

82. Forefront was at all times fully aware of its obligation to protect the PII and PHI of its patients.

83. Forefront was also aware of the significant repercussions that would result from its failure to do so.

E. Defendants Fail to Comply with Industry Standards

84. As noted above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

85. Several best practices have been identified that a minimum should be implemented

by healthcare providers like Defendants, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

86. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards.

87. The Center for Internet Security (CIS) released its *Critical Security Controls*, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[25]

88. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

89. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in

[25] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited February 15, 2022).

reasonable cybersecurity readiness.

90. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and in the healthcare administrative services industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

F. Forefront's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

91. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

92. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical and administrative components.

93. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*.

94. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Forefront left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

95. Ransomware attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which

compromises the security or privacy of the PHI."[26]

96. Forefront's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

G. Forefront's Conduct Breached Its Obligations to Its Patients and Employees.

97. Forefront breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

98. Forefront's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, ransomware and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in

[26] *See* 45 C.F.R. 164.40.

violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low

probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

o. Failing to adhere to industry standards for cybersecurity.

99. As the result of, among other things, maintaining computer systems in dire need of security upgrading, *see* Notice of Data Incident, Forefront negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

100. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

101. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Forefront.

H. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

102. Cyberattacks and data breaches at healthcare providers like Forefront are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

103. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[27]

104. That is because any victim of a data breach is exposed to serious ramifications

[27] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited February 15, 2022).

regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

105. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and to harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim.

106. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

107. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit and correcting their credit reports.[28]

108. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

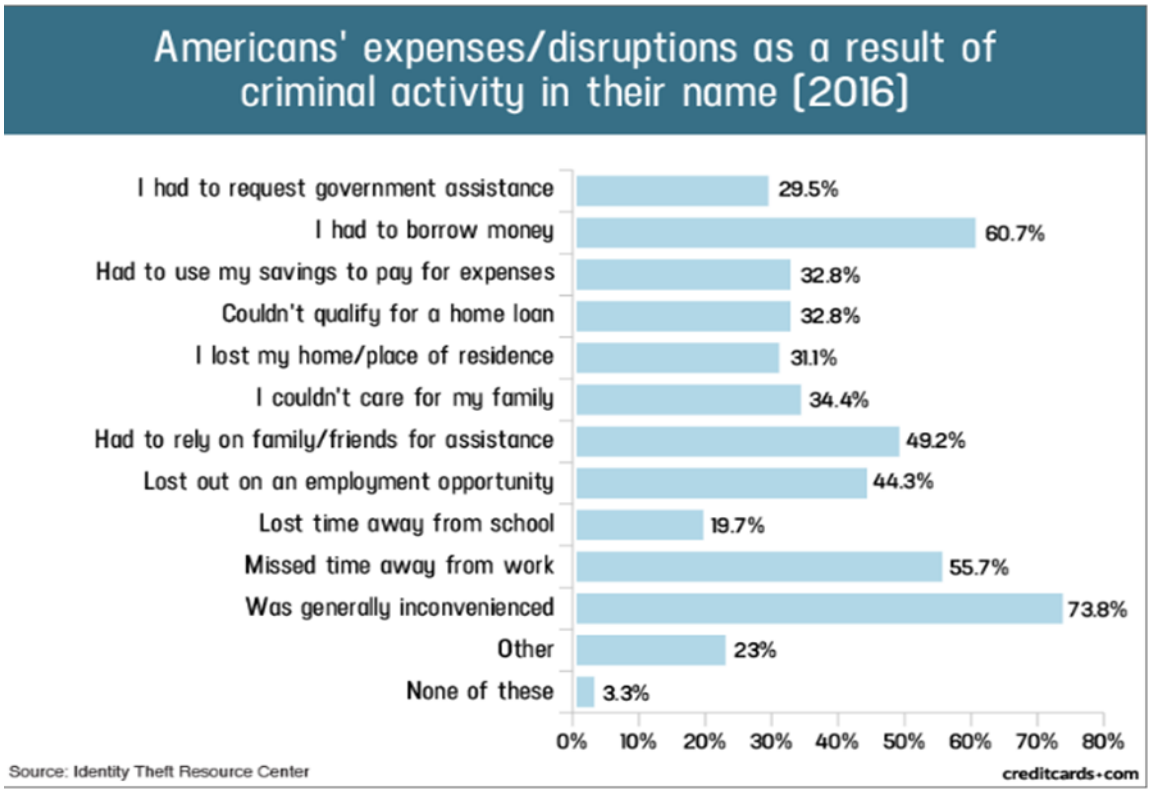
---

[28] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited February 16, 2022).

109. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

110. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

111. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[29]



[29] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

112. Moreover, theft of Private Information is also gravely serious, as PII/PHI is an extremely valuable property right.[30]

113. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

114. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[31]

115. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

116. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

117. According to the GAO Report:

---

30 *See, e.g.*, John T. Soma, *et al*., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

31 *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited February 16, 2022).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at 29.

118. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

119. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

120. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

121. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[32] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

122. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[33] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social

---

[32] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[33] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited February 16, 2022).

Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[34]

123. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

124. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

125. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[36]

126. Medical information is especially valuable to identity thieves.

127. According to account monitoring company LogDog, coveted Social Security

---

34 *Id.* at 4.

35 Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

36 Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[37] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[38]

128. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

129. For this reason, Forefront knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Forefront was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

I. Plaintiffs' Experiences

Plaintiff Leitermann

130. In or about July 2021, Plaintiff Leitermann received a notice letter from Defendants informing her that her Private Information was compromised in the Data Breach. The letter instructed Plaintiff Leitermann to spend time mitigating her potential damages, including by "review[ing] the statements you receive from your healthcare providers and health insurance plan."

132. As a result of the Data Breach, Plaintiff Leitermann has experienced an increase in the number of spam phone calls, emails and texts since the Data Breach, which appear to be placed with the intent of obtaining personal information to commit identity theft by way of a social engineering attack.

133. Accordingly, as a result of the Data Breach, and pursuant to Defendant's own instructions set forth in the Notice of Data Breach, Plaintiff Leitermann was required to, and did

---

[37] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[38] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

in fact, spend time monitoring her accounts and statements for suspicious activity.

134. In response to the Notice of Data Breach, Plaintiff Leitermann spent time dealing with the consequences of the Data Breach, which included and will include time spent verifying the legitimacy of the *Notice of Data Breach*, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

135. Plaintiff Leitermann is very careful about sharing her Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

136. Plaintiff Leitermann stores any and all documents containing Private Information in a safe and secure location and shreds any documents he receives in the mail that contain any Private Information, or that may contain any information that could otherwise be used to compromise her financial accounts and identity. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

137. Plaintiff Leitermann suffered actual injury and damages as a result of the Data Breach. Implied in the purchase of dermatology services from Defendants was the requirement that it adequately safeguard her PII. Plaintiff Leitermann would not have paid Defendants for dermatology services had Defendants disclosed that they lacked data security practices adequate to safeguard the Private Information.

138. Plaintiff Leitermann suffered actual injury in the form of damages and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendants for the purpose of purchasing dermatology services, which was compromised by the Data Breach.

139. Plaintiff Leitermann suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

140. Plaintiff Leitermann has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen Private Information being placed in the hands of unauthorized third-parties and possibly criminals.

141. Plaintiff Leitermann has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Anderson's Experience

142. On or about July 8, 2021, Forefront sent Plaintiff Anderson, and Plaintiff Anderson subsequently received, a letter identifying that her Private Information may have been impacted by the Data Breach.

143. After receiving the breach notification letter, Plaintiff Anderson estimates that she has spent in excess of 100 hours taking steps to determine if she has been subjected to fraud as a result of the Data Breach, and to prevent potential fraud or identity theft.

144. She has taken (and continues to regularly take) steps to remove her personal information from and opt out of public websites so that her name does not turn up in internet search engine search results, out of concern for her publicly available information being used in connection with the stolen Private Information to commit fraud or identity theft against her.

145. Plaintiff Anderson has also been monitoring her bank and credit card statements and has gone through these statements in detail to see if she had been subjected to any fraudulent charges. Plaintiff has also been vigilant in monitoring her credit since the Data Breach.

146. Plaintiff Anderson suffered actual injury and damages as a result of the Data

Breach. Implied in her relationship with Forefront was the requirement that it adequately safeguard her Private Information. Plaintiff Anderson would not have transacted with Forefront had it disclosed that it lacked data security practices adequate to safeguard her Private Information.

147. Plaintiff Anderson suffered actual injury in the form of damages and diminution in the value of her Private Information—a form of intangible property that she entrusted to Forefront.

148. Plaintiff Anderson suffered lost time, invasion of her medical privacy, loss of value of her Private Information, and inconvenience as a result of the Data Breach.

149. Plaintiff Anderson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

150. Plaintiff Anderson has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Forefront's possession, is protected and safeguarded from future breaches.

Plaintiff Kunzelmann's Experience

151. On or about July 9, 2021, Plaintiff Kunzelmann received an email from Forefront disclosing that "a data security incident that may have involved some of your data" has occurred.

152. As a result of the Data Breach, Plaintiff Kunzelmann has had to take steps to secure his Private Information. Plaintiff Kunzelmann has continued monitoring bank statements, credit card statements, and other financial information since being informed of the Data Breach.

153. Plaintiff Kunzelmann suffered actual injury and damages as a result of the Data Breach. Implied in the purchase of dermatology services from Defendants was the requirement that it adequately safeguard his PII. Plaintiff Kunzelmann would not have paid Defendants for dermatology services had Defendants disclosed that they lacked data security practices adequate

to safeguard the Private Information.

154. Plaintiff Kunzelmann suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendants for the purpose of purchasing dermatology services, which was compromised by the Data Breach.

155. Plaintiff Kunzelmann suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

156. Plaintiff Kunzelmann has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

157. Plaintiff Kunzelmann has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Forefront's possession, is protected and safeguarded from future breaches.

J. Plaintiffs' and Class Members' Damages

158. To date, Defendants have done virtually nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

159. The complimentary fraud and identity monitoring service offered by Forefront is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

160. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

161. Plaintiffs' PII and PHI was compromised as a direct and proximate result of the Data Breach.

162. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

163. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

164. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud and similar identity theft.

165. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, ransomware and other illegal schemes based on their Private Information.

166. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees and similar costs directly or indirectly related to the Data Breach.

167. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach.

168. Numerous courts have recognized the propriety of loss of value damages in related cases.

169. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Forefront was intended to be used by Defendants to fund adequate security of Forefront's computer

property and to protect Plaintiffs' and Class Members' Private Information. In short, Plaintiffs and the Class Members did not get what they paid for.

170. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

171. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges, insurance claims and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts and credit reports for unauthorized activity for years to come.

172. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants (in some form), is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected and that such data is properly encrypted.

173. Further, as a result of Forefront's conduct, Plaintiffs and Class Members are forced

to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

174. As a direct and proximate result of Forefront's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

175. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs seek certification of the following classes of persons defined as follows:

> **National Class:** All persons impacted by the Forefront Data Breach, including all persons who were sent a notice of the Forefront Data Breach.
>
> **Patient Subclass:** All patients of Forefront impacted by the Forefront Data Breach, including all patients of Forefront who were sent a notice of the Forefront Data Breach.
>
> **Employee Subclass:** All employees and former employees of Forefront impacted by the Forefront Data Breach, including all employees and former employees of Forefront who were sent a notice of the Forefront Data Breach.

Excluded from the Classes are any judges presiding over this matter and court personnel assigned to this case.

176. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, the Classes reportedly include approximately 2,413,553 current and former patients and employees of Forefront. The identities of Class Members are ascertainable through Forefront's records, Class Members' records, publication notice, self-identification and other means.

177. **Commonality**. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common

questions of law and fact include, without limitation:

a. Whether Forefront unlawfully used, maintained, lost or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Forefront failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Forefront's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA;

d. Whether Forefront's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Forefront owed a duty to Class Members to safeguard their Private Information;

f. Whether Forefront breached its duty to Class Members to safeguard their Private Information;

g. Whether hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Forefront knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Forefront's misconduct;

j. Whether Forefront's conduct was negligent;

k. Whether Forefront's conduct violated federal law;

l. Whether Forefront's conduct violated state law and

m. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages and/or injunctive relief.

178. Common sources of evidence may also be used to demonstrate Forefront's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Forefront's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

179. **Typicality**. Plaintiffs' claims are typical of the claims of the respective Class they seek to represent, in that the named Plaintiffs and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests adverse to the interests of the other members of the Class.

180. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions, including data privacy litigation of this kind.

181. **Predominance**. Forefront has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

182. **Superiority**. A Class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Forefront. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

183. Forefront has acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

184. Certification is appropriate because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Forefront owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing and safeguarding their Private Information;

b. Whether Forefront's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Forefront's failure to institute adequate protective security measures amounted to negligence;

d. Whether Forefront failed to take commercially reasonable steps to safeguard consumer Private Information and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

185. Finally, all members of the proposed Classes are readily ascertainable. Forefront has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Forefront.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE
(On Behalf of Plaintiffs and the Classes)

186. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

187. Plaintiffs bring this claim individually and on behalf of the Class Members.

188. In order to receive medical treatments and services, or as a condition of employment, Forefront and/or their affiliates required Plaintiffs and Class Members to submit non-public Private Information, such as PII and PHI.

189. Plaintiffs and Class Members entrusted their Private Information to Forefront and/or their affiliates with the understanding that Forefront would safeguard their information.

190. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Forefront and its affiliates had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft.

191. Forefront's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give

prompt notice to those affected in the case of a data breach.

192. Forefront owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

193. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Forefront and its client patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law.

194. Forefront was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

195. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

196. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

197. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

198. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

199. Defendants breached their duties and thus were negligent by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Forefront include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Failing to adequately train its employees to recognize and contain phishing attacks;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

200. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

201. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

202. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

203. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

204. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) continue to provide adequate credit and identity monitoring to all Class Members.

COUNT II

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Classes)

205. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

206. Through their course of conduct, Defendants, Plaintiffs, and Class Members entered into implied contracts for either the provision of healthcare and treatment or as a condition of their employment with Defendant, as well as implied contracts for Defendants to implement data security adequate to safeguard and to protect the privacy of Plaintiffs' and Class Members' Private Information.

207. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendants when they first went for medical care and treatment at one of Defendants' facilities or when they were required to provide their PII to Defendants as a condition of their employment with Defendants.

208. On information and belief, at all relevant times, Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiffs and Class Members that they would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

209. Implicit in the agreement between Plaintiffs and Class Members and the Defendants to provide Private Information, was the latter's obligation to: (a) use such Private Information for

business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

210. When Plaintiffs and Class Members provided their Private Information to Defendants and/or their affiliates in exchange for medical services or employment, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

211. Defendants and/or their agents solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices.

212. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

213. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

214. Class Members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

215. The protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts for healthcare services and/or employment.

216. The implied contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized and embodied in certain documents, including (among other documents) Defendants' Privacy Policy and Notice of Data Incident.

217. Similarly, the implied contract to adequately safeguard employees Private Information is acknowledge, memorialized and embodied in certain documents, including (among other documents), Defendants' Notice of Privacy Practices that Defendants provide to all employees.

218. Defendants' express representations, including, but not limited to, the express representations found in its Privacy Policy and Notice of Privacy Practices, memorializes and embodies the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and to protect the privacy of Plaintiffs' and Class Members' Private Information.

219. Consumers of healthcare value their privacy, the privacy of their dependents and the ability to keep their Private Information associated with obtaining healthcare private. To consumers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

220. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants and/or their affiliates and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendants in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

221. A meeting of the minds occurred as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendants and/or their Agents and paid for the provided healthcare or labor in exchange for, amongst other things, either the provision of health care or employment in conjunction with the protection of their Private Information.

222. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

223. Defendants materially breached their contractual obligation to protect the non-public Private Information Defendants gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

224. Defendants materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Policy.

225. Forefront did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and approximately 2,413,553 Class Members.

226. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

227. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

228. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received health care or employment that was of a diminished value to that described in the contracts.

229. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare or employment with data security protection they should have received and the healthcare or employment with diminished data security protection they received.

230. Had Defendants disclosed that their security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members nor any reasonable person would have purchased healthcare or sought employment from Defendants and/or their affiliated healthcare providers.

231. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

232. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

233. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

COUNT III

UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Classes)

234. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

235. This count is pleaded in the alternative to the breach of contract count above.

236. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and/or their Agents and in so doing provided Defendants with their Private Information.

237. In exchange, Plaintiffs and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

238. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

239. The amount Plaintiffs and Class Members paid for goods and services were used, in part, to pay for use of Defendants' network and the administrative costs of data management and security.

240. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

241. Defendants failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members

provided.

242. Defendants acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

243. Had Plaintiffs and Class Members known that Defendants had not reasonably secured their Private Information, they would not have agreed to Defendants' services.

244. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury as set forth herein.

245. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

COUNT IV

BREACH OF FIDCUIARY DUTY
(On Behalf of Plaintiffs and the Patient Subclass)

246. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

247. Forefront occupied a position of advisor or counselor to its patients and employees such that Forefront Dermatology would reasonably inspire confidence that it would act in good faith and in the best interest of its patients and employees. Accordingly, a fiduciary relationship exists between Forefront and its patients and/or employees, including Plaintiffs and Class Members.

248. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and/or their Agents and in so doing provided Defendants with their Private Information.

249. By failing to implement and maintain reasonable safeguards to protect their PII, failing to comply with industry-standard data security practices, failing to disclose critical information regarding the nature and extent of the Data Breach, and allowing a third-party hacker to release their PII on the dark web, Forefront intentionally or negligently failed to act in good faith and solely for the benefit of Plaintiffs and Class Members.

250. Forefront's failure to act solely for the benefit of Plaintiffs and Class Members was a real and meaningful factor in bringing about their injuries.

251. As a direct and proximate result of Forefront's breach of fiduciary duty, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as described herein, or, alternatively, Plaintiffs and Class Members seek an award of nominal damages.

COUNT V

BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Classes)

252. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

253. Defendants required Plaintiffs and Class Member to provide their Private Information as a condition of treatment and/or for purposes of employment. Such information was highly personal, sensitive, and not generally known.

254. Defendants expressly and implicitly agreed to protect the confidentiality and security of the Private Information it collected, stored, and maintained.

255. Defendants disclosed the Private Information to unauthorized third parties by failing to implement and maintain reasonable safeguards to protect its patients' and employees' Private Information and failing to comply with industry-standard data security practices.

256. As a direct and proximate result of Forefront's breach of confidence, Plaintiffs and

Class Members suffered injury and sustained actual losses and damages as described herein, or, alternatively, Plaintiffs and Class Members seek an award of nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs JUDITH LEITERMANN, LYNN ANDERSON, and MILAN E. KUNZELMANN, individually and behalf of all others similarly situated, pray for relief as against FOREFRONT DERMATOLOGY, S.C. and FOREFRONT MANAGEMENT, LLC as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23, appointing Plaintiffs as Class Representatives and the undersigned attorneys as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to ensure that the Class has an effective remedy, including enjoining Forefront from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action and

F. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

DATED: February 28, 2022

Respectfully submitted,

/s/ Tina Wolfson
Tina Wolfson

twolfson@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Tel: (310) 474-9111
Fax: (310) 474-8585

Andrew W. Ferich
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Gary M. Klinger
gklinger@masonllp.com
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (202) 429-2290

Interim Co-Lead Class Counsel for Plaintiffs and the Proposed Class

Stephen R. Basser (WIED No. 121590)
sbasser@barrack.com
Samuel M. Ward (WIED No. 216562)
sward@barrack.com
BARRACK, RODOS & BACINE
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

Interim Executive Committee Chair for Plaintiffs and the Proposed Class